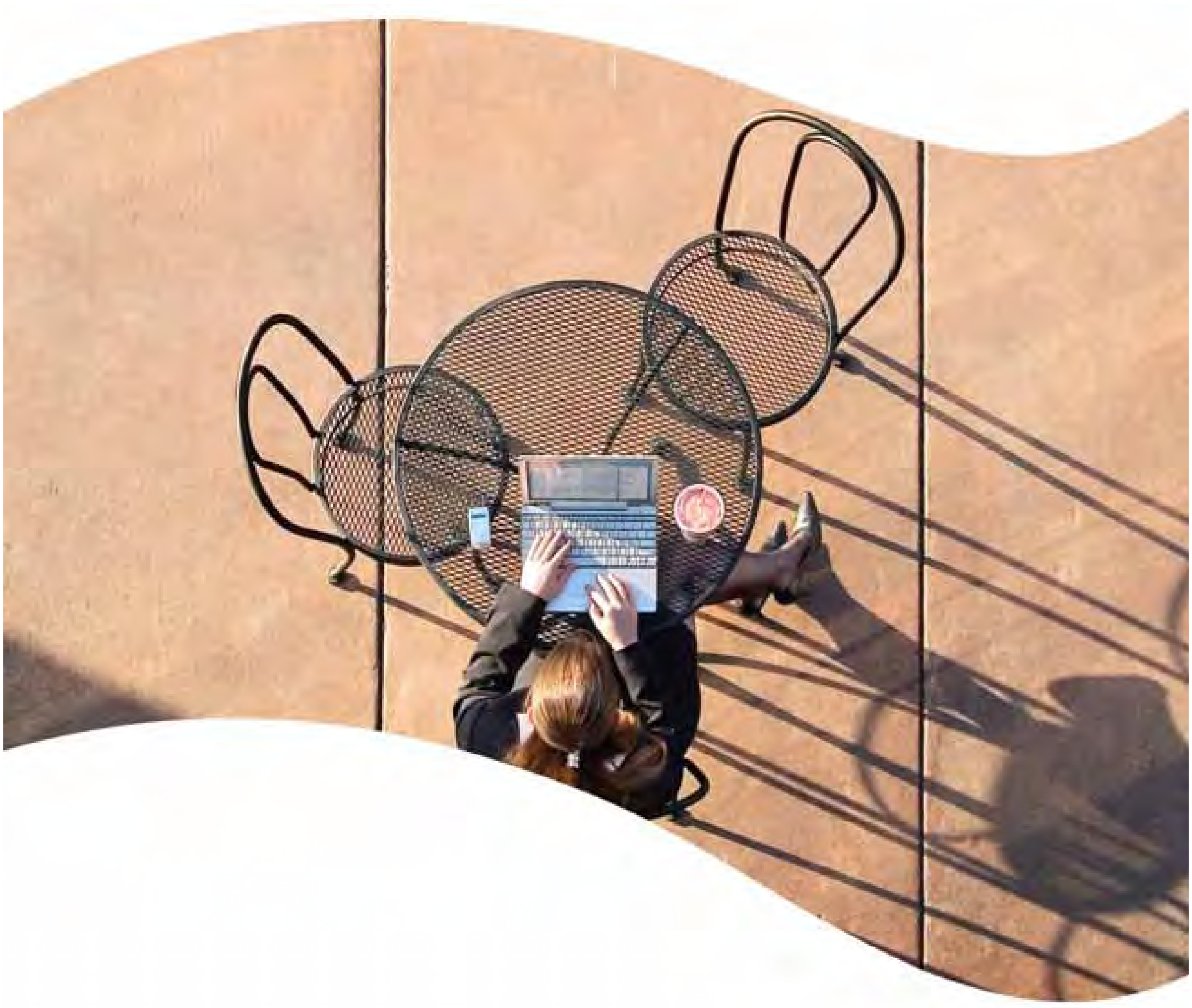
COMPREHENSIVE INTERNET SECURITY™

SonicWALL Email Security 5.0 User's Guide

SONICWALL



SonicWALL® Email Security User's Guide

Version **5.0**

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale, CA 94089-1306
Phone: +1.408.745.9600
Fax: +1.408.745.9300
E-mail: info@sonicwall.com

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

NOTE**:** The SonicWALL Email Security software service is an annual subscription which is subject to the terms and conditions of SonicWALL, Inc.’s applicable subscription agreement and includes:

Product updates, SonicWALL threat signature updates, and standard technical support for one (1) year from the date of purchase.

SonicWALL Email Security appliances are integrated hardware and software solutions, which include SonicWALL Email Security software. SonicWALL Email Security appliances are subject to the terms and conditions of SonicWALL, Inc.’s applicable license agreement. Updates to the SonicWALL Email Security software, SonicWALL Spam Signature Updates, and technical support may be purchased on an annual basis. AntiVirus support is optionally available.

Table of Contents

Preface

SonicWALL Email Security guards the perimeter of the organization against the costly, dangerous, and growing threats to corporate email. Threats are stopped before they infiltrate corporate mail servers and employee inboxes. SonicWALL Email Security secures email connections and blocks unwanted email while ensuring timely delivery of all legitimate email. SonicWALL Email Security provides the most comprehensive and effective spam blocking available. The solution filters email uniquely for each user, taking into accounts the varying preferences and patterns of each user.

SonicWALL's solution is dynamic, self-learning, and self-running. SonicWALL Email Security provides protection against all forms of email threats from entering your Inbox.

Documentation Overview

SonicWALL provides documents to install, administer, and use its products to protect email users from phishing, spam, viruses; and manage your security policies for your organization.

Who Should Read this?	Document Name
Network Administrators	SonicWALL Email Security Getting Started Guide SonicWALL Email Security Administrator Guide
Email Users	SonicWALL Email Security User Guide

Note To view SonicWALL Email Security documentation online, go to: http://www.sonicwall.com/support/

Documentation Conventions

Font	Meaning
Bold	Terms you see in a SonicWALL Email Security window
Italic	Variable names
`Courier`	Text on a command line
`Bold Courier`	Text that you type in a command line

Finding Online Help



Clicking the Help button describes how to use the contents of the window.

Note IMPORTANT: Configure your web browser's pop-up blockers to allow pop-ups from your organization's SonicWALL Email Security server before using SonicWALL Email Security, because many of the windows are pop-up windows.

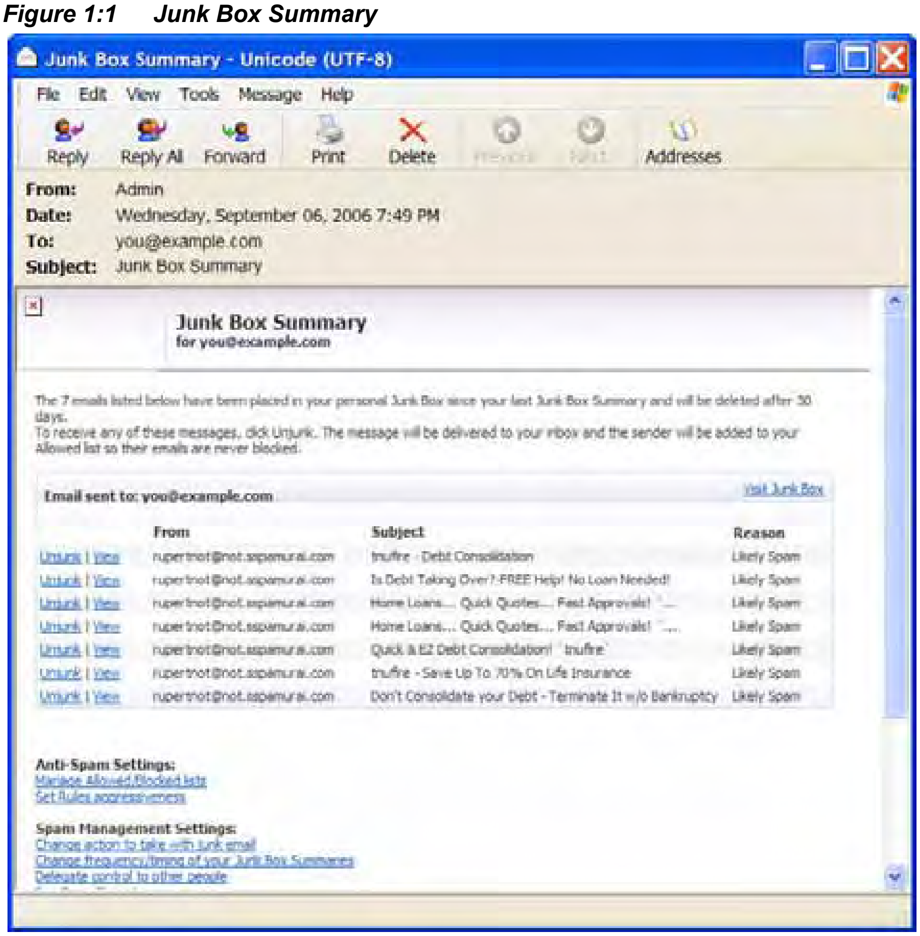
CHAPTER 1

About SonicWALL Email Security

When A Message is Flagged as Junk

When SonicWALL Email Security determines a message is junk, it stores it in a Junk Box. Your network administrator determines whether users can access their Junk Boxes. If configured, the software periodically sends you email messages listing the messages flagged as junk email.

Figure 1:1 Junk Box Summary



You can scan these messages to see if there are any messages you want to receive, which were miscategorized as Junk. If you see a message you want to receive, click the Unjunk link next to it and the message is sent to your Inbox. The sender of any messages that you unjunk is added to your list of allowed senders and their messages are not marked as junk in the future.

Depending on the settings for your organization's installation of SonicWALL Email Security, you might also have a View link in the Junk Box summary message. Click the link to view the contents of the message to assist in determining whether it is spam.

Deleting Spam

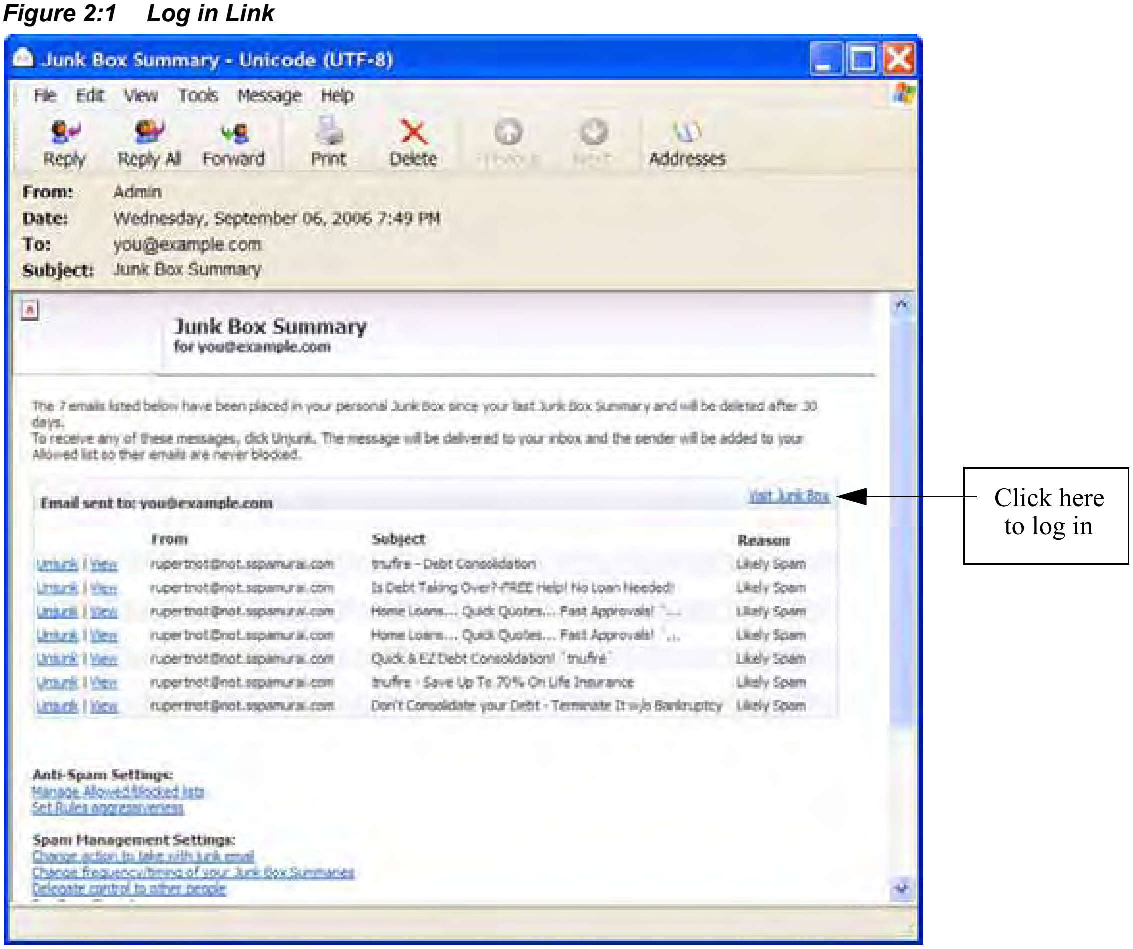
If you do not care about the messages in the Junk Box, you can leave them there. They are automatically deleted later.

CHAPTER 2

Logging In to Your Junk Box

When SonicWALL Email Security determines that a message contains a threat or a likely threat, it stores the message in a Junk Box on the server and alerts you by email, as shown in Figure 2:1. You can log in to your Junk Box to view messages that were junked by SonicWALL Email Security. Log in to SonicWALL Email Security using the link that your IT administrator gave you or by clicking the link in the Junk Box Summary message you receive.

Figure 2:1 Log in Link



Note IMPORTANT: Configure your web browser's pop-up blockers to allow pop-ups from your organization's SonicWALL Email Security server before using SonicWALL Email Security, because many of the windows are pop-up windows.

To log in to your Junk Box:

1. Log in with your user name and password.
   The Login Window is shown in Figure 2:2.

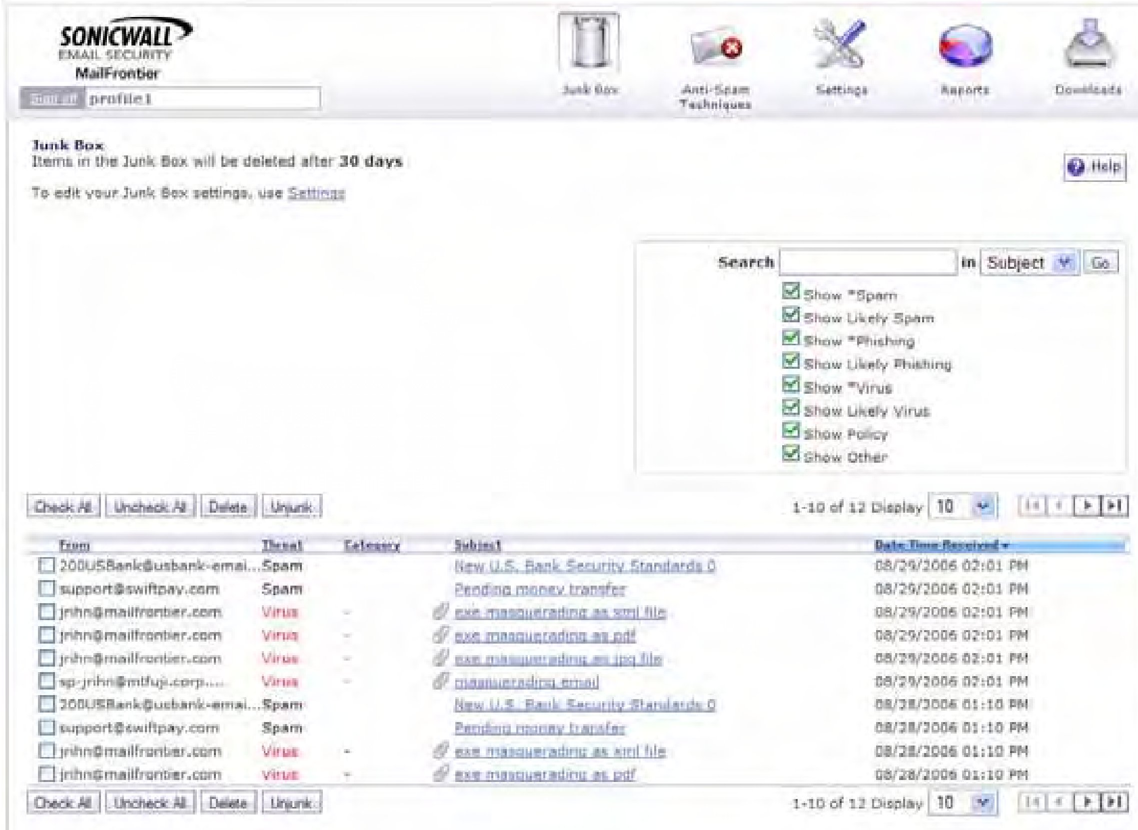
Figure 2:2 Login Window



2. Choose the appropriate domain from the list, if necessary.

   Your personal Junk Box appears, with any messages that have been flagged as spam or other unwanted email, as shown in Figure 2:3.

Figure 2:3 Junk Box window



You can display all junk mail, likely junk mail, or other unwanted email if your organization has configured SonicWALL Email Security to screen for viruses, phishing, or email that contains content your organization has chosen to manage through policies.



Searching in Your Junk Box

To search for email messages in your Junk Box:

1. Enter a word or partial word in the Search text box.
   Note: Search is not case-sensitive.
2. Select the field you want to search in (Subject, From, or Date).
   Date formats can be entered as MM/DD/YY or MM/DD/YYYY.
3. Click **Go**.

To search for specific email threats, check or deselect check boxes under the Search text box and click Go. As an example, suppose you wanted to see only messages that were Spam or Likely Spam. To do this, select the **Show *Spam** and **Show Likely Spam** check boxes, deselect all other check boxes and click **Go**.

Deleting Messages

To delete individual messages:

1. Select a message.
2. Click **Delete**.

To delete all messages:

1. Click **Check All**.
2. Click **Delete**.

If you do nothing, these messages are automatically deleted after the number of days configured by the SonicWALL Email Security administrator.

Unjunking Messages

To unjunk a message:

1. Click the box to the left of the message to select the message you want to retrieve.
2. Click **Unjunk**.

   The senders of any messages you unjunk are added to your list of allowed senders; future messages from these senders are delivered directly to your Inbox.

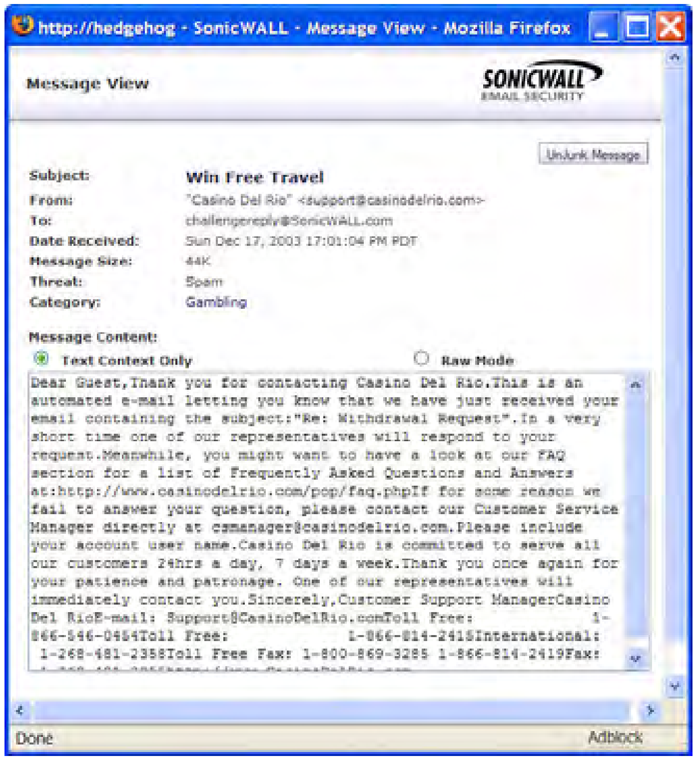
To unjunk all messages:

1. Click **Check All**.
2. Click **Unjunk**.

Viewing Message Content

Depending on your organization’s configuration, you can view the message content by clicking the View link in the Junk Summary Message. For security reasons, SonicWALL Email Security displays only the text portions of the message and does not display graphical images.

Figure 2:4 Viewing the Message

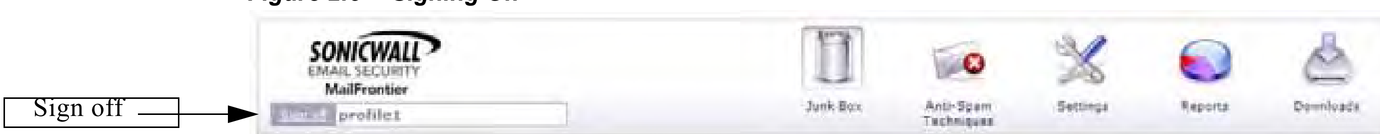


To view the header information, click the **Raw Mode** option.

Ending Your Junk Box Session

When you are done managing your Junk Box, click the **Sign Off** button in the upper left corner of the screen or close the browser window.

Figure 2:5 Signing Off



CHAPTER 3
Anti-Spam Techniques

Managing Allowed and Blocked Lists

Use the Anti-Spam Techniques window to create your own lists of senders from whom you want to allow and block email. SonicWALL Email Security provides separate lists for people, companies (domains), and mailing lists. For each type of list, click the **Allowed** and **Blocked** tabs to see the different allowed and blocked lists.

You can search for allowed and blocked names, company, and lists in the Anti-Spam Techniques window. Click **Search** and type the name of the person, company, or list.

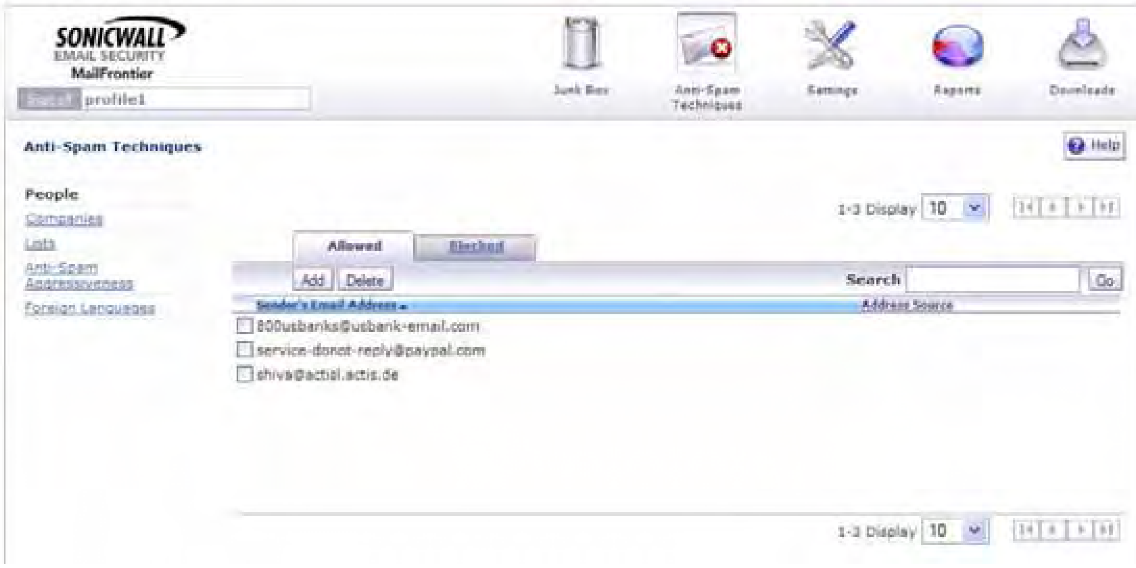
Note An email address or domain cannot be simultaneously on the Allowed and Blocked lists. If you add an address in one list that already exists on the other, SonicWALL Email Security removes the address from the first list.

Adding People to the Allowed or Blocked Lists

To add people to Allowed or Blocked lists:

1. Click the **Anti-Spam Techniques** button. The window in Figure 3:1 appears.

Figure 3:1 Anti-Spam Techniques



2. Click **Allowed** to add people to the Allowed list.

3. Click **Add** to add a person.
   The Add Sender to Allowed List dialog appears.

Figure 3:2 Figure 11 Add People to Allowed List



4. Enter the email address of the address you want to allow.
   If you add multiple people, press Enter after each one.
5. Click **Add**.

Deleting People from the Allowed or Blocked Lists

To delete people from Allowed or Blocked lists:

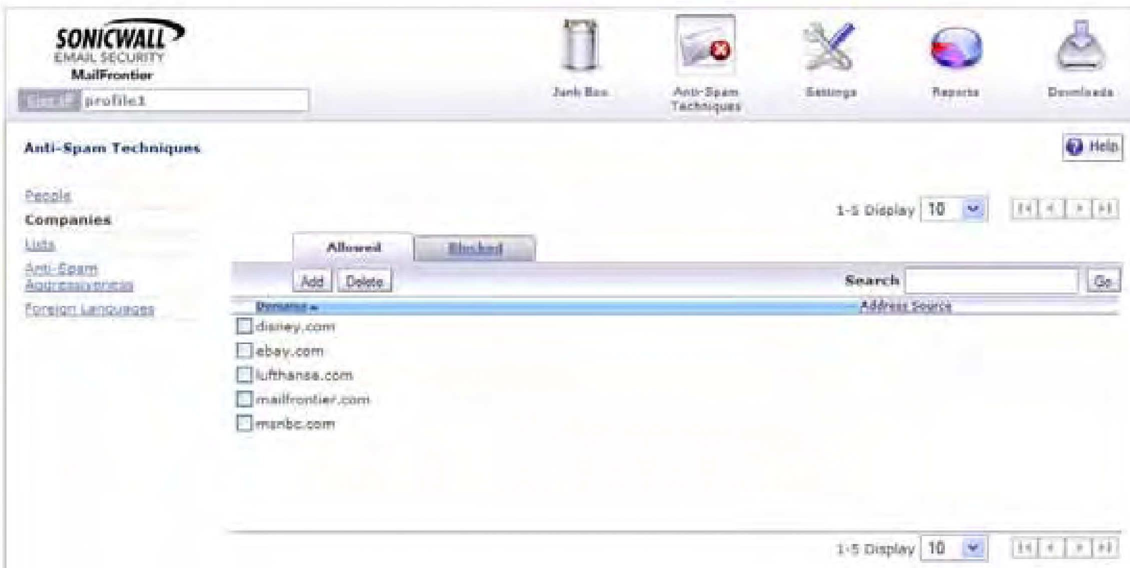
1. Click the **Anti-Spam Techniques** button.
2. Click the checkbox adjacent to the address to delete that address from the Allowed list.
3. Click **Delete**.

Adding Companies or Domains to the Allowed or Blocked Lists

To add companies or domains to Allowed or Blocked lists:

1. Click the **Anti-Spam Techniques** button.
2. Click **Companies** from the left hand navigation menu.
   A list of companies is displayed, as shown in Figure 3:3.

Figure 3:3 Allowing or Blocking Companies and Domains



Note Some company addresses are adjacent to a dimmed checkbox. These addresses are on the organization Allowed list; users cannot delete these companies.

3. Click **Allowed** to view the companies and domains in the Allowed list.

Adding a Company or Domain to the Allowed List

To enter the name of the company or domain into your allowed list, perform the following:

1. Click the **Add** button.

Figure 3:4 Add Companies to Allowed List



2. Enter the Web address you want to allow.
   If you add multiple addresses, press Enter after each one.

Note NOTE: Specify full domain names in this format: example.com or example.gov. Domain names such as .gov or .com, are not valid entries.

3. Click **Add** to add a company or domain.

Deleting a Company or Domain

To delete a company or domain:

1. Check the check box adjacent to the name of the company or domain you want to delete.
2. Click the **Delete** button to delete that company from the Allowed list.

Adding Lists to the Allowed List

Email messages from mailing-list servers do not always come from the same email address or FROM: field in the address. The email messages are from the person who posted the message to the list-server and the message is to (TO) the mailing list. The list sections looks at both the FROM: and TO: fields and allows only mailing-list mail.

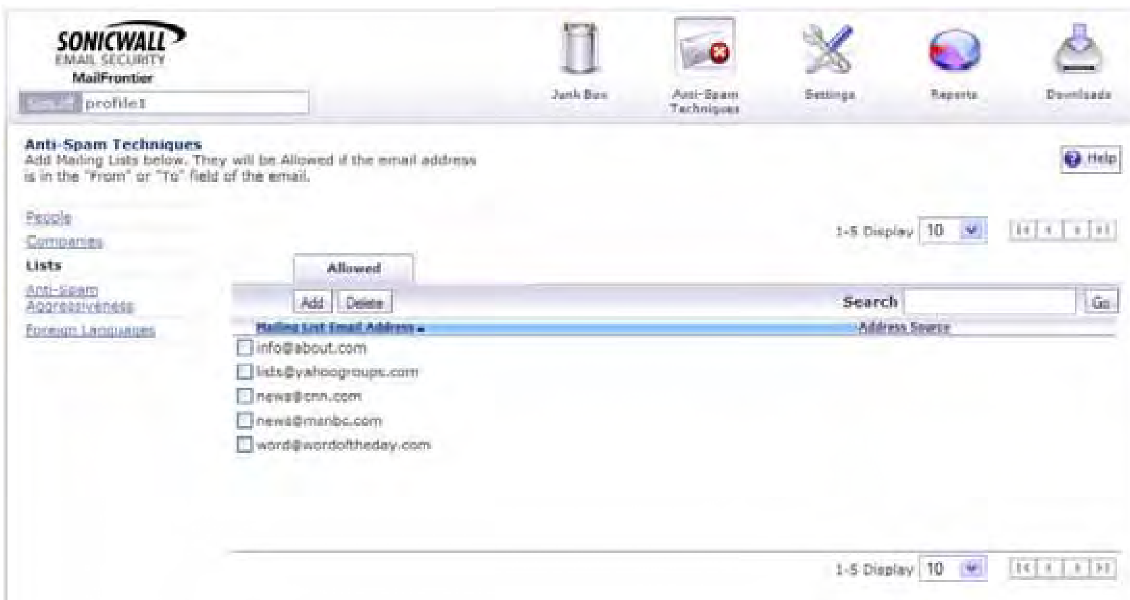
Note You can only add and delete Allowed lists.

To add lists to Allowed Lists:

1. Click the **Anti-Spam Techniques** button.
2. Click the **Lists** link.

   The Lists window appears, as shown in Figure 3:5.

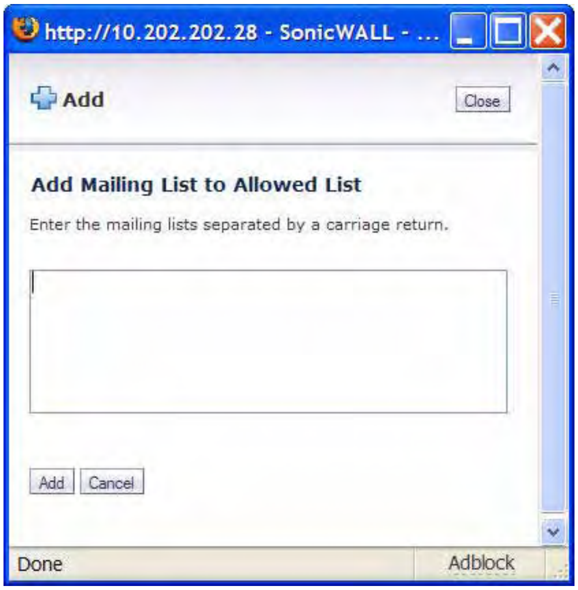
Figure 3:5 Allowed Lists



3. Click **Add** to add mailing lists to Allowed Lists.

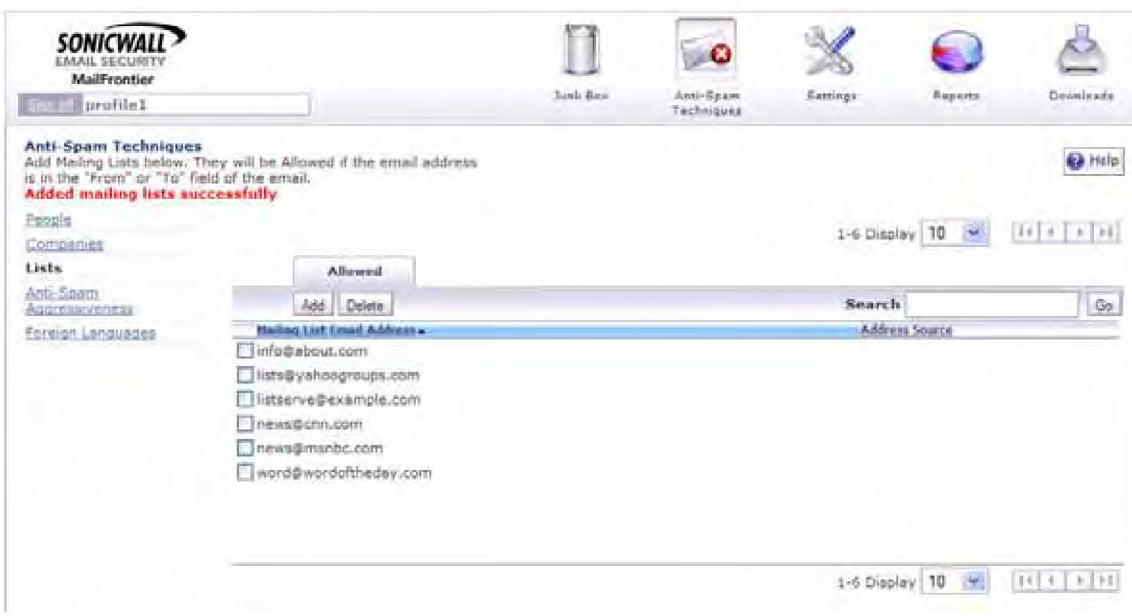
   The Add Lists window appears, as shown in Figure 3:6.

Figure 3:6 Add Lists to Allowed List



4. Enter the addresses of the lists.
5. Enter a carriage return between each list.
6. Click **Add**.
   The updated Allowed Lists window appears, as shown in Figure 3:7.

Figure 3:7 Updated Allowed Lists Window

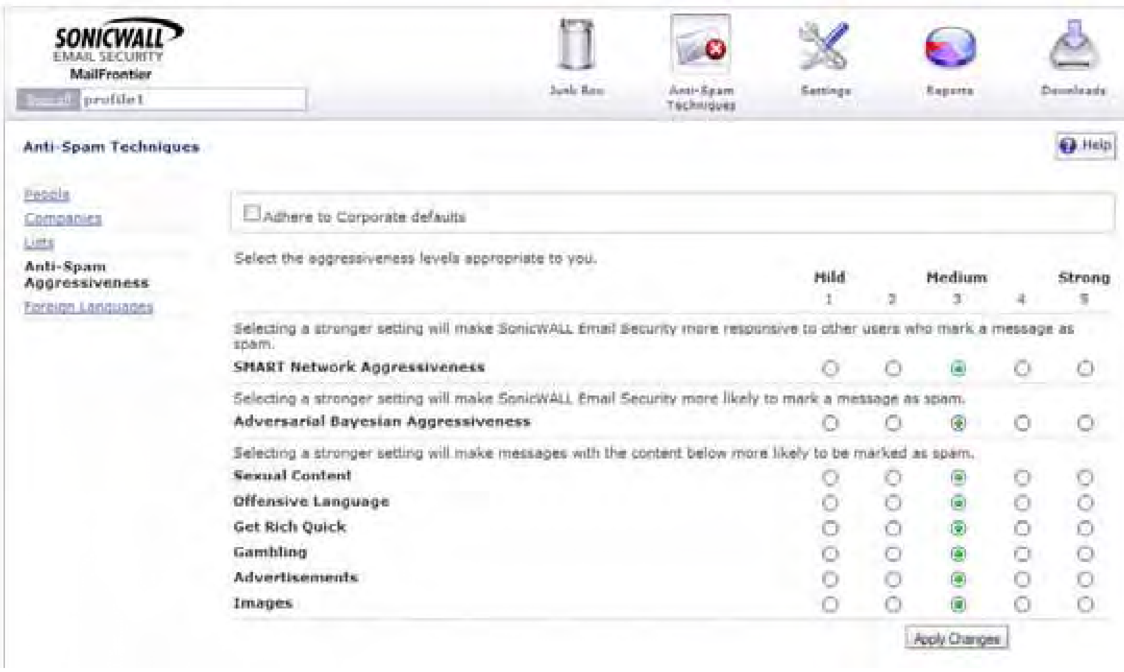


Configuring Anti-Spam Aggressiveness

The Anti-Spam Aggressiveness window allows you tailor SonicWALL Email Security to your preferences. This window is optional. SonicWALL recommends using the default setting of Medium or 3 unless you require different settings for specific types of spam blocking.

Note The Adhere to Corporate/Group Defaults checkbox allows you to follow your IT department's recommendations. If your IT department enforces these settings, the checkbox is dimmed; you cannot change blocking levels.

Figure 3:8 Anti-Spam Aggressiveness Settings



Configuring SMART Network Aggressiveness Settings

You can adjust the SMART Network Aggressiveness settings to customize the level of influence community input has on organization spam blocking, produced by the Self-Monitoring Active Response Team (SMART) network. Updates are provided to your gateway server at defined intervals.

To adjust your collaborative settings, click one of the radio buttons from Mild (1) to Strong (5). A setting of 5 means that you are comfortable with the collective experience of the SonicWALL user community. A setting of 1 or 2 indicates that you are skeptical of the collective experience and want to judge more email for yourself.

Configuring Adversarial Bayesian Aggressiveness Settings

This aggressiveness setting determines how likely an email message is to be identified as junk email. This is the foundational setting for the Bayesian statistical contribution to spam blocking. Selecting a stronger setting makes SonicWALL Gateway more likely to mark a message as spam.

Determining Amounts and Flavors of Spam

You can determine how aggressively to block particular types of spam, including sexual content, offensive language, get rich quick, gambling, and advertisements.

For each of the spam flavors:

- Choose Mild (checkbox 1) to be able to view email that contains terms that relate to these topics.
- Choose Medium (checkbox 2 through 4) to cause SonicWALL Email Security to tag this email as likely junk.
- Choose Strong (checkbox 5) make it more likely that email with this content is junked.

Screening Messages in Other Languages

The Foreign Languages window allows you to use the language in which a message is written as a criteria for receiving the message.

For each language shown in Figure 3:9, you can choose allow, block, or have no opinion. For example, you might want to receive all messages in German, but want to block messages in another language. You might also have no opinion about receiving messages in other languages.

Figure 3:9 Foreign Language



For each language, decide if you want to receive or block messages in that language.

- To receive all messages in a language, click the button under Allow All adjacent to the language.
- To block all messages in a language, click the button under Block All adjacent to the language.

Click **No Opinion** for a language to receive messages in that language. All messages in languages for which you choose No Opinion are screened for spam and all other filters in SonicWALL Email Security.

Note English is not included on the list of foreign languages because it is the default language for SonicWALL Email Security.

Configuring Language Preferences for SonicWALL Email Security

You can change the language in which the user interface for SonicWALL Email Security is displayed.

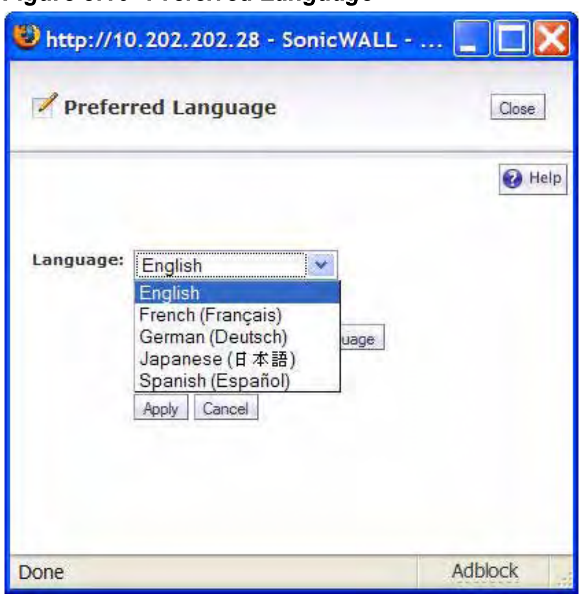
To change the language:

1. Click the **Preferred Language** link in the lower right frame of most user interface windows.



The Preferred Language window appears, as shown in Figure 3:10.

Figure 3:10 Preferred Language



2. Click the Language drop-down list.
3. Select any of the available languages.

Note Your computer must support the language so that the language is displayed correctly.

Click **Reset** to Browser Primary Language to return to the language your browser usually runs.

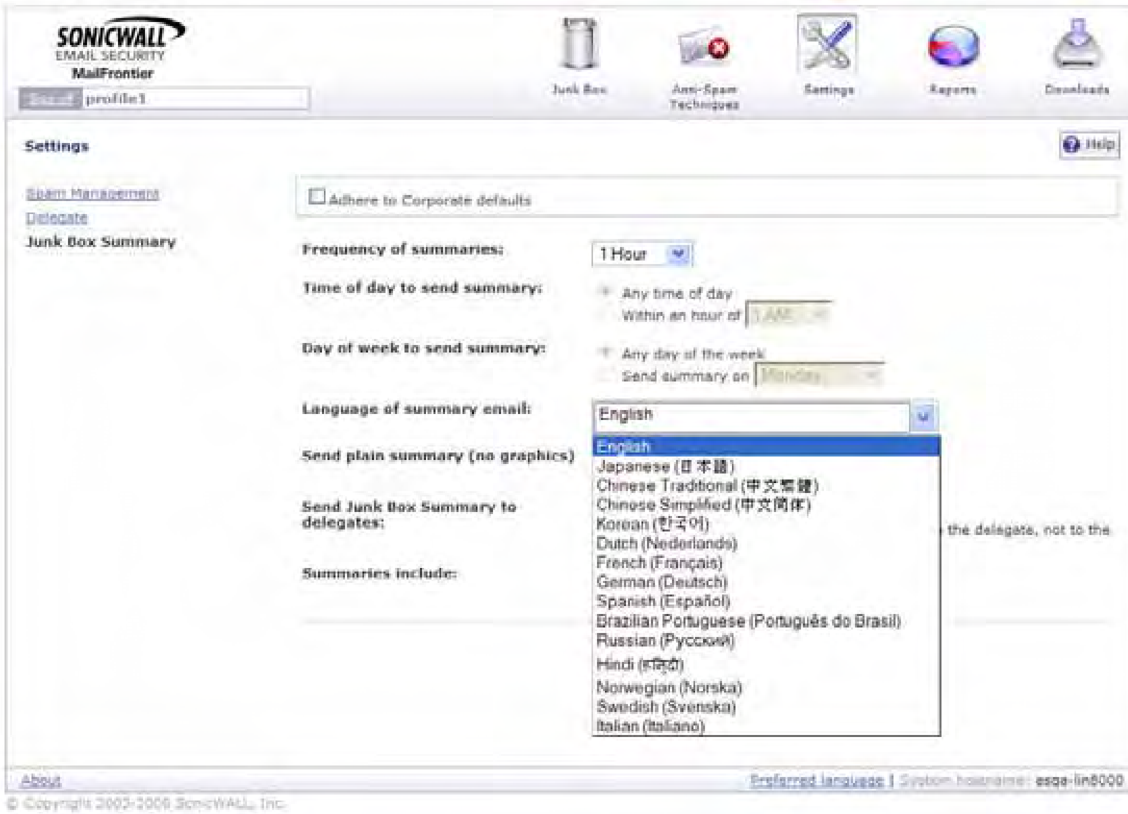
Configuring Language Preferences for your Junk Box Summary

You can configure your Junk Box summary to appear in any of the languages shown in Figure 3:11, if your computer supports the language modules to display the character sets.

To change the language for your Junk Box summary:

1. Click the **Settings** icon at the top of the window and select the **Junk Box Summary** link.
2. Select a language from the **Language of summary email** drop-down list, as shown in Figure 3:11.

Figure 3:11 Languages for Junk Box Summaries



3. Click Apply.

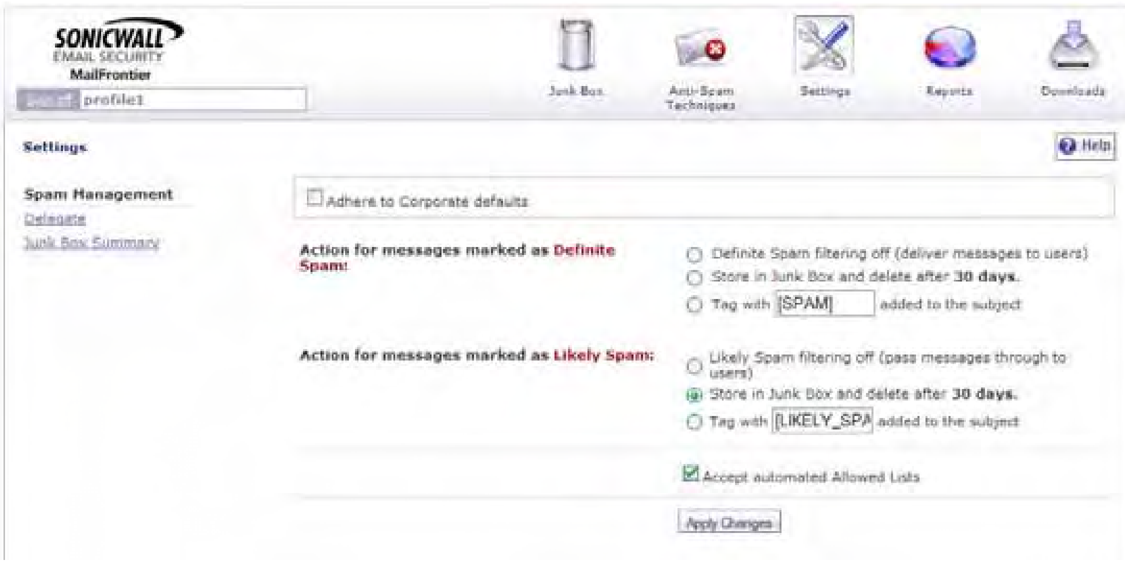
CHAPTER 4

Settings

Settings allows you to set various options about what you want to do with messages that are spam, likely spam, phishing, viruses, or have content that is not allowed by your organization's policy.

Click the **Settings** button to view and change your spam-filtering settings.

Figure 4:1 Settings window



Spam Management

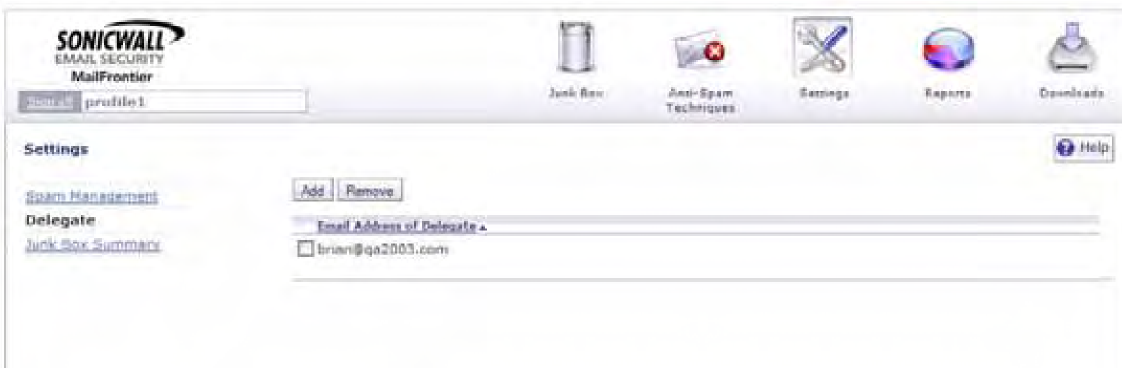
You can determine what action to take with messages marked as Spam and Likely Spam. Check one of the following options:

Spam Filtering Off:	SonicWALL Email Security passes messages through to your Inbox
Store in Junk Box and delete after number of days:	SonicWALL Email Security stores all messages that it determines as spam for the number of days set by your SonicWALL Email Security administrator.
Tag with text:	you can add words to mark messages that are spam or are likely spam.

Assigning Delegates for the Junk Box

The Delegate window allows you to authorize one or more users to monitor your Junk Box, as shown in Figure 4:2.

Figure 4:2 Delegate User



To add a delegate:

1. Click the **Add** button.
   The Add New Delegate screen appears, as shown in Figure 4:3.

Figure 4:3 Add New Delegate



2. Select a delegate from the list.

   If there are too many users to display, to search for the user, type the user's name in the text box and click **Go**.
3. Enter the email address of the delegate in the textbox.
4. Click the checkbox adjacent to the preferred delegate.
5. Click **Add Delegate**.

Removing a Delegate

To remove a delegate:

1. Click the delegate that you want to remove.
2. Click the **Remove** button in the Delegate window.

Junk Box Summary

When SonicWALL Email Security moves junk and likely junk messages to your Junk Box, you can choose to be notified periodically by email.

Figure 4:4 Junk Summary Settings



To manage your junk summary settings:

1. Choose the default email frequency for Junk summaries from the drop-down list. Your choices range from never to 14 days.
2. Choose the Time of day to receive the Junk summary.
3. Choose the Day of the week to receive the Junk summary.

4. Choose the Language in which to view your Junk summary. You can choose to view the your junk summaries in the following languages:
   - English
   - Japanese
   - Chinese Traditional
   - Chinese Modern
   - Korean
   - Dutch
   - French
   - German
   - Spanish
   - Brazilian Portuguese
   - Russian
   - Hindi
   - Norwegian
   - Swedish
   - Italian

Note To correctly display the Junk Summary in a language other than English, you must install the appropriate language packs on your computer.

5. If you prefer, check the **Plain Summary** (no graphics) checkbox.
6. Check the **Send Junk Box Summary to delegates** checkbox if you want to send summaries to a delegate. If you have not yet assigned a delegate, navigate to the **Settings > Delegate** page.
7. Choose one of the options for the junk summary:
   - All junk messages
   - Only likely junk
8. Click **Apply**.

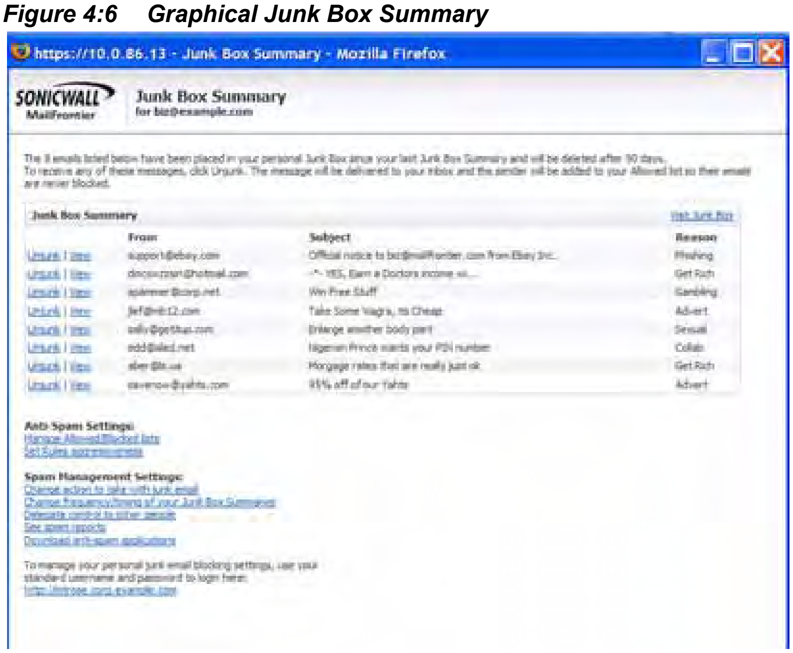
Send Simple (no graphics) Summary or Graphical Summary

You can receive the Junk Box Summary as a simple list or in a more graphical format. Figure 4:5 shows a simple list; Figure 4:6 shows a more graphical presentation.

Figure 4:5 Simple Junk Box Summary



Figure 4:6 Graphical Junk Box Summary



CHAPTER 5

Reports

The reports in this module show statistics for your organization—not just your own spam. Click the **Reports** button to view them.

SonicWALL Email Security displays summary information about the emails processed, how many were junk, and why they were flagged as junk.

Figure 5:1 Reports

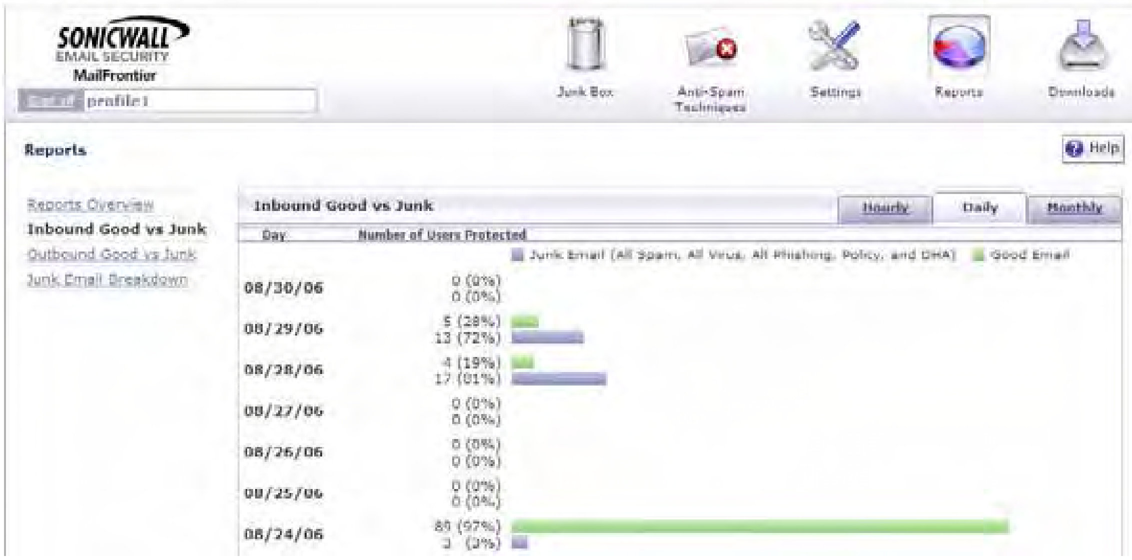


Select the report you want to view by clicking the appropriate link to the left. Each report allows you to select the time frame for which you want the report run: hourly, daily, or monthly.

Inbound Good vs. Junk Email

The Inbound Good vs. Junk page illustrates the number of incoming email that is good versus junk email. Values are shown in number of messages per day and also according to the percentage of good versus junk.

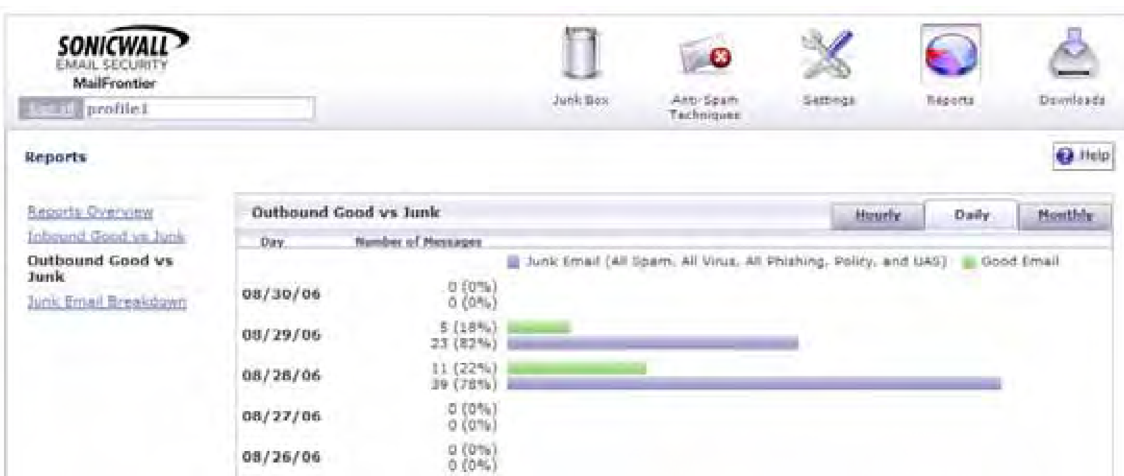
Figure 5:2 Inbound Good vs. Junk



Outbound Good vs. Junk Email

The Outbound Good vs. Junk page illustrates the number of outgoing email that is good versus junk email. Values are shown in number of messages per day and also according to the percentage of good versus junk.

Figure 5:3 Outbound Good vs. Junk



Junk Email Breakdown

The Junk Email Breakdown page illustrates the types of messages received, and shows the comparative amounts of messages that were identified as spam, likely spam, contained viruses, likely contained viruses, phishing, likely phishing, were identified by policy rules, and were considered Directory Harvest Attacks (DHA).

Figure 5:4 Junk Email Breakdown



Index

SonicWALL,Inc.
1143 Borregas Avenue T: 408.745.9600 www.sonicwall.com
Sunnyvale,CA 94089-1306 F: 408.745.9300

P/N 232-000699-00
08/06